HIPAA - Privacy Rule and Clarity Voice VoIP Services

What is Health Information Portability and Accountability Act (HIPAA)?

The Office for Civil Rights enforces:

- the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information,
- the HIPAA Security Rule, which sets national standards for the security of electronic protected health information,
- and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety

What is HIPAA Compliance?

HIPAA sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed.

This includes covered entities (CE), anyone who provides treatment, payment and operations in healthcare, and business associates (BA), anyone with access to patient information and provides support in treatment, payment or operations. Subcontractors, or business associates of business associates, must also be in compliance.

The HIPAA Privacy Rule addresses the saving, accessing and sharing of medical and personal information of any individual, while the HIPAA Security Rule more specifically outlines national security standards to protect health data created, received, maintained or transmitted electronically, also known as electronic protected health information (ePHI).

A supplemental act was passed in 2009 called The Health Information Technology for Economic and Clinical Health (HITECH) Act which supports the enforcement of HIPAA requirements by raising the penalties of health organizations that violate HIPAA Privacy and Security Rules. The HITECH Act was formed in response to health technology development and increased use, storage and transmittal of electronic health information.

And the HIPAA/HITECH Act Omnibus Rule from 2013 which amended the HIPAA/HITECH Act Privacy, Security, Breach Notification, and Enforcement Rules.

Clarity Voice's solution ensures that customer calls and fax messages are secure with encryption in transit and at-rest, along with other features, protecting patient data and guarding against unauthorized access to protected health information.

Is Clarity Voice required to comply with HIPPA Privacy Rules?

By the definitions noted above Clarity Voice is neither a covered entity or a business associate and is covered by the **conduit exception rule**. The HIPAA conduit exception rule is only applicable to providers of purely conduit services who do not have access to protected health information (PHI) other than infrequently or randomly. For this reason, conduit providers do not have to sign a Business Associate Agreement.

Specific justification of the applicability of the conduit exception rule is cited in the Federal Register / Vol. 78, No. 17 / Friday, January 25, 2013 / Rules and Regulations:

> *As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to protected health information would not qualify the company as a business associate.*

While this is our legal counsel perspective, Clarity has gone further to help ensure privacy and regulatory requirements are met related to data and security.

Can a covered entity or business associate use the Clarity's voice and e-fax services and remain HIPAA compliant?

Please consult with an attorney as to whether your use of our service may involve the transmission, receipt, or storage of ePHI.

The following outline of our systems architecture and functionality is for informational purposes only and is not intended to provide legal advice.

Clarity has implemented the following safeguards to support various regulations and compliance:

VOICE DATA:

- Our multiple Data Centers are designed to be compliant
    - Iron Mountain Data Center - HIPAA – PCI – FISMA High – FedRAMP – SOC 2 Type 2 – SOC 3 – ISO 27001 – ISO 50001 – ISO 14001 – ISO 9001
    - 123Net Data Center - HIPAA, PCI-DSS, and SSAE-18 SOC 2 Type II/SOC 3 compliant
- Data is stored securely (in the sense that we require authentication for access and access provided to only those who need it to do their job)
- All systems are behind firewalls
- All Data is stored securely and behind a firewall
- Customer data that could provide ePHI are encrypted during all transmissions (voice is configurable)
- All in and out data transport are secured through appropriate levels of encryption
- All passwords are encrypted and regularly requested to be reset by users
- System access is restricted to only authorized users that maintain our systems
- Automatic logoff features are implemented on all systems
- Any customer choosing to use call recording functionality is set to purge automatically after 30 days and likewise access to these files are permission based at an individual user

- Seven distinct layers of physical and data security between endpoints
    - Data securely stored
    - Application layer security
    - Endpoint security
    - Network security
    - Perimeter and other layers of physical security
    - Policy management thru SOPs
    - Monitoring

FAX DATA:

- Our eFax platform utilizes HTTPS technology for transmitting fax traffic internally.
- All fax caching is purged following successful transmission; aka we do not store any fax documents.
- Furthermore, our fax servers are secured behind a firewall and access is restricted to our system administrators.

SMS/MMS DATA

- Any SMS messages sent outside our servers are NOT guaranteed to be compliant.

CLARITY VOICE EMPLOYEES & VENDOR/PARTNERS

- Employees and company vendor/partners are required to comply with federal CPNI (Customer Propriety Network Information) privacy requirements which governs Clarity's employers, agents, partners access and use of customer data.
- Clarity is required by the Federal Communications Commission (FCC) to file a CPNI certification affidavit annually with the FCC.

Secure management of protected health information is your topmost priority. That's why Clarity Voice provides a multilayered security model, so voice and fax communications are protected and meet privacy and regulatory requirements.